SIMM 85B
Telework Security Standard

December 21, 2009

Table of Contents

Telework Security Standard

Applicability

This standard is not to be construed as either replacing or superseding any other applicable statewide, federal or private industry security policy, standard or requirement including, but not limited to, State Administrative Manual section 5100, and sections 5300 through 5399.

This standard applies to telework users who have access to California state IT infrastructure and information assets through public networks. In addition to telework users, this standard is applicable to security, system, and network engineers and administrators, as well as computer security program managers, who are responsible for the technical aspects of preparing, operating, and securing remote access solutions and telework client devices, and agency heads and program managers responsible for the overall security of information assets within their agencies.

The material in this standard is technically oriented, and it is assumed that readers have at least a basic understanding of remote access, networking, network security, and system security. Those not having this level of understanding should consult their agency Chief Information Officer and Information Security Officers for assistance.

Definitions[1]

Agency – When used lower case (agency), refers to any office, department, board, bureau, commission or other organizational entity within state government. When capitalized (Agency), the term refers to one of the state's super agencies such as the State and Consumer Services Agency or the Health and Human Services Agency. (From State Administrative Manual (SAM) Section 4819.2, Definitions)

Direct Application Access Architecture – A high-level remote access architecture that allows teleworkers to access an individual application directly, without using remote access software.

Information Assets – All categories of information (confidential, personal, sensitive, or public), all forms of information assets (paper or electronic), information technology facilities, equipment and software owned or leased by state agencies. (See SAM Section 4989.1, Definitions; *Condensed*).

IT Administrators – The agency's IT staff such as those individuals responsible for support and security of the IT infrastructure.

[1] The National Institute of Standards and Technology (NIST) Special Publication 800-46, Appendix A Glossary is the source of remote architecture definitions.

IT Infrastructure – An agency's information technology platform for the support of agency programs and management. Included in the infrastructure are equipment, software, communication networks. (See SAM Section 4989.1, Definitions; *Adapted.*)

Multi-homed connection - A host connected to two or more networks or having two or more network addresses. For example, a computer may be connected to a serial line and a LAN or to multiple LANs.

Network-level Connection – The connection provides access to a state private network through a tunneling or a remote desktop access architecture and the software and data that reside on the internal information assets**.**

Portal Architecture – A high-level remote access architecture that is based on a server that offers teleworkers access to one or more applications through a single, centralized interface.

Remote Access - The connection of an information asset from an off-site location to an information asset on state IT infrastructure.

Remote Desktop Access Architecture – A high-level remote access architecture that gives a teleworker the ability to remotely control a particular desktop computer at the organization, most often the computer assigned to the user that resides at the organization's office from a telework device.

Split Tunneling - The process of allowing a remote VPN user to access a public network, most commonly the Internet, at the same time that the user is allowed to access resources on the VPN. A disadvantage of this method is that it essentially renders the VPN vulnerable to attack as it is accessible through the public, non-secure network.

Strong password – A minimum of eight characters using a combination of upper and lowercase letters, numbers and special characters.

Telework – An arrangement in which an employee regularly performs officially assigned duties at home or an alternate work site.

Tunneling Architecture – A high-level remote access architecture that provides a secure tunnel between a telework device and a tunneling server through which application traffic may pass. Tunnels use cryptography to protect the confidentiality and integrity of the transmitted information between client device and the VPN gateway

Two-factor authentication – Authentication based on two of the following: something you know (i.e., password), something you have (i.e., token or smartcard), or something you are (i.e., a biometric).

Virtual Private Network (VPN) – A virtual network, built on top of existing physical networks, that provides a secure communications tunnel for data and other information transmitted between networks.

Web-based Connection – the connection provides access to one or more applications through a single centralized interface through a direct application access or portal architecture (typically a web-browser to a portal server located within the demilitarized zone [DMZ]). This type of connection creates an area that serves as a boundary between two or more networks and isolates the information asset from the internal private network.

Agency Head Requirements

Training of Telework Users

Before authorizing employees to connect to state IT infrastructure for telework purposes, agency heads shall ensure that managers, supervisors, and telework users receive security training addressing at least the following subjects:

- The responsibilities outlined in this standard;
- The potential enterprise risks to both the agency's information assets and the information assets of other government entities that are interconnected and/or available to authorized users through the agency's IT infrastructure;
- The potential risks to employees if an exception is made to authorize the use of personally-owned information assets and the agency's limitations on guidance and support of personally-owned information assets;
- How information is to be backed up and destroyed, including cache clearing and telework document shredding in the telework setting;
- Protection of remote access-specific authenticators, such as passwords, personal identification numbers (PIN), and hardware tokens;
- Recognition of social engineering attack techniques and appropriate mitigation measures;
- The consequences for disabling, altering or circumventing the security configurations that protect state information assets; and
- Security incident management and breach disclosure procedures.

Agency Management Requirements

Identify the Needs of Telework Users

Before managers and/or supervisors authorize work to be performed under a telework arrangement they must do the following:

- Identify the type of work to be performed through the telework arrangement.
- Only authorize telework user access to resources which are necessary to carry out the telework arrangement safely and securely. Managers and/or supervisors shall consider whether the needs to support the telework arrangement can be met with less access and connectivity than provided at the main office. Work to be performed during an emergency situation to maintain essential operations may not warrant the telework user to have the same access or connectivity as they do at the main office. In many cases, a telephone and email access through a Web-based connection may be all that is required.

- Ensure a telework agreement between the telework user and manager is signed and maintained in the agency file. (Reference the [Date] Statewide Telework Model Policy at http://www.dgs.ca.gov/Telework/Resources.htm)

Agency IT Administrator Requirements

Agency IT Administrators shall ensure that the control requirements which are applied to telework users of ***both*** state-owned and personally-owned information assets are in place before connections to state IT infrastructure are allowed. In addition, before connections are made, agency IT Administrators shall ensure that the following requirements are met:

Maintain Software Updates

Agency IT Administrators shall ensure that information assets used to connect to the agency IT infrastructure are checked and use up-to-date operating system software and security software (anti-virus, anti-spyware, firewall, and host intrusion prevention) every time a remote connection is initiated. This is typically accomplished through a Network Access Control (NAC) solution which integrates an automatic remediation process that fixes a non-compliant information asset before allowing access into the network systems. This ensures the information asset is operating securely before interoperability with agency IT infrastructure is allowed.

Limiting Telework User Privileges

- Each telework user shall have an individual user account that does not have elevated privileges. Accounts with elevated privileges create an increased security risk because they allow the user to change security settings and install applications.
- Telework user accounts shall require two-factor authentication, except when using a Web-based connection, such as Outlook Web Access (OWA) or other similar interface.
- Telework user accounts shall, as a rule, be set up to have limited privileges. Telework users will not normally require accounts with full privileges (i.e., administrative accounts). In the unusual event that telework users require administrative accounts, they shall be used only when performing authorized IT Administrator tasks, such as installing updates and application software, managing user accounts, and modifying operating system and application settings on the information asset.

Validating Control Requirements

- Agency IT Administrators shall log and monitor all telework access. Log files shall capture sufficient detail to allow a virtual reconstruction of the end-to-end network session. This level of detail will be necessary in the event of a breach or malware infection.
- Agency IT Administrators shall periodically assess the controls on personally-owned information assets used to connect to State IT infrastructure.

Telework User Requirements

State-owned Information Assets to be Used for Network-Level Connections

Telework users shall ensure that all computing equipment which is connected to the state IT infrastructure network for telework purposes are state-owned information assets which have been configured in accordance with secure enterprise and agency standard configurations, including those set forth herein. Telework users shall not connect personally-owned information assets to the state IT infrastructure at the network-level unless an approved written exception applies and is implemented in accordance with the additional standards which apply to use of personally-owned information assets herein.

Web-based Connections

Telework users that connect to state IT infrastructure without network-level access, such as utilizing a web browser to connect to authorized Internet-facing infrastructures (e.g., Citrix, web-based applications, Outlook Web Access) need not initiate connections from state-owned information assets.

Secure Connections

Telework users shall only connect to state IT infrastructure through secure encrypted channels that are authorized by agency management. These channels may include encrypted virtual private networks (VPNs), encrypted web access, encrypted broadband and encrypted dial-up connections. At no time may the telework user initiate two simultaneous connections to different networks (e.g., no split tunneling and no multi-homed connection).

Maintaining Security of Information Assets Used for Telework

Just as in the agency main office, security measures cover not only information systems and technology, but all aspects of the information and information systems used by the employee, including paper files, other media, storage devices, and telecommunications equipment (e.g., laptops, Personal Digital Assistants [PDAs], Blackberries and smart cell phones) used in the course of work. Employees must keep government property and information safe, secure, and separated from their personal property and information.

Further, telework users shall adhere to all other information security policies, standards and procedures, regarding the use of state information assets, regardless of the work location including not disabling, altering or circumventing established security controls on state information assets used to connect to state IT infrastructure, such as antivirus and antispyware software, personal firewalls, content filtering software and automatic updates.

Protection From Unauthorized Physical Access

Telework users shall ensure that information assets used to telework or connect to state IT infrastructure are physically secured. Telework users must implement the following controls:

- Protecting information assets from unauthorized access and use by others, including family members, friends and other visitors.
- Leaving information assets only in secured locations (e.g., locked cabinet or drawer, locked rooms in locked buildings as applicable and in accordance with the state entity's

information handling policies and procedures) and not in unattended vehicles or other locations where they may be easily stolen.

- Using additional physical security controls, such as locking the telework device to a stationary object (e.g., desk or chair) with a computer cable lock, where appropriate.
- Using agency approved encryption software to ensure sensitive, personal, and/or confidential information is stored and transmitted securely and not accessible by unauthorized individuals.
- Using and securely maintaining (e.g. not written-down or shared with anyone) strong passwords for all information assets that can be set up to restrict access with a password.

Standards for Exceptions When a Personally-Owned Information Asset is Used to Telework

Exception and Risk Approval Process

In the rare situation where it is not possible to use state-owned information assets to establish a network-level connection in order to telework, the agency head, in consultation with the agency Chief Information Officer (CIO) and Information Security Officer (ISO), will consider the increased risk to the state, the agency, and the telework user posed by the telework user connecting to state IT infrastructure with personally-owned information assets. There is increased risk with use of personally-owned information assets because, unlike state information assets, they are not managed by IT Administrators dedicated specifically to perform the necessary maintenance. These risks may include, but are not limited to, unauthorized access to other government agency information assets, the comingling of agency information with individual's personal information on personally-owned information assets which must be made available in the litigation hold and e-discovery, public disclosure, and audit processes.

If the agency Head chooses to accept the risk, then the personally-owned information assets authorized for use in a telework arrangement must be configured and operated in accordance with the requirements that apply to state-owned assets, and the additional requirements below. The exception and risk approval shall be in writing and maintained for at least two years following the termination of the telework arrangement.

Telework users who require assistance in making the configuration changes necessary to meet the following requirements to their personal computing assets may need to seek the assistance of professional computer support/repair services at their own expense. The US-CERT online reading room provides free less technical resources to assist individuals with securing their personal computers and home networks. These are available at: http://www.us-cert.gov/reading_room/before_you_plug_in.html

Additional Training Requirements

Agency Management must provide specialized training for telework users who are authorized to use personally-owned information assets to connect to state IT infrastructure in order to educate the user on how to take the security precautions outlined below, including performing software updates and disabling unneeded application features.

User Account Passwords

Each telework user account shall have a strong password to prevent unauthorized access through password guessing, password cracking software, and other similar techniques used to compromise the telework user account.

Networking Configuration

Telework users shall ensure that their personally-owned information assets are configured to limit network access, including:

- Ensure the firewall software included with the computer is turned on and set to block all incoming connections from other computers and outside sources on the Internet.
- Disabling non-essential services, such as file and print sharing.
- Disabling unneeded networking features such as wireless network access features (e.g., IEEE 802.11a/b/g/n, Bluetooth, and infrared);
- Limiting the use of remote access utilities (e.g., for remote technical support) and configuring the information asset to require the remote person to be authenticated before gaining access to the information asset; and
- Configuring information assets so that they do not automatically attempt to join wireless networks they detect.

Attack Prevention

Telework users shall ensure that a combination of software and software features are installed and operating on their information assets in order to prevent attacks, including:

- Antivirus and antispyware software;
- Personal firewalls that deny all types of communications that users have not specifically approved as being permitted; and
- Content filtering software.

Maintain Software Updates

Telework users shall ensure that manufacturer recommended security updates and configuration changes are applied regularly to the software on their information assets. Manufacturer's will usually release updates for their products following the discovery of a vulnerability. Telework users must watch for critical notices and periodic reminders from the manufacturer and agency about the availability of security updates that fix discovered vulnerabilities, and take the actions necessary to apply the security update within the required timeframe so that the telework user's personally-owned information asset is correctly maintained and conforms to these standards. In addition to the operating system, updates shall, at a minimum be applied to the following types of software as soon as they become available:

- Web browsers (program that facilitates access to the Internet, such as Internet Explorer, Mozilla Firefox, etc.);
- Email clients (software and a service that facilitates email communication, such as Outlook, Lotus Notes, etc.);

- Instant messaging clients (software and a service that facilitates instant voice chat and text chat communications and file sharing, such as AIM, ICQ, Jabber, etc.);
- Antivirus and antispyware software (software that detects and blocks malicious code);
- Personal firewalls (software and/or hardware that allows the user to define access policies for inbound connections to the computer they are protecting and outbound services the computer is authorized to access); and
- Content filtering software (software that blocks access to certain websites and services).

Telework users shall review manufacturer documentation for each software program their information asset contains in these categories to determine each program's update capabilities and enable automatic updates where possible.

Secure Application Configurations

Telework users shall configure their applications (typically this can be accomplished through the "Tools" and "Options" in the application, though it may vary by manufacturer and application) to decrease risk and to support security, including:

Generally:

- Disabling unneeded application features and configuring applications to stop or block activity that is likely to be malicious (the more applications installed and application features enabled the greater the security risk and maintenance responsibility);
- Avoiding downloading and installing software if the software is not provided by either the agency, the information asset's manufacturer or a reputable vendor.

Web browsers:

- Restricting Web browser cookies (small data files created by a Web server that is stored on the computer either temporarily for that session only [session cookie] or permanently on the hard disk [persistent cookie]. Cookies are a concern because they can be set to store personal information, including user login ids and passwords).
- Blocking pop-up windows (a small window that is displayed on top of an existing open window or application);
- Enabling phishing (type of scam) filtering (software that can detect specific patterns in email as a potential scam and either delete or send to a folder for further review) capabilities;
- Removing unneeded browser plug-ins (a small program that enhances the capabilities of a larger software program, usually associated with image editing, or audio or video programs);
- Protecting sensitive information stored by the browser (e.g., passwords);
- Preventing website passwords from being saved by the browser and recalled automatically during the logon process; and
- Running browsers with the fewest privileges possible by limiting options and disabling unnecessary features, (e.g., disabling Java© and JavaScript, disabling pop-ups and not loading images automatically).

Email clients:

- Preventing automatic loading of remote email images;
- Limiting mobile code execution (e.g., disabling Active X, Java© and Javascript where possible);
- Setting default message reading format and sending format to plain text;
- Disabling automatic previewing and opening of email messages; and
- Enabling spam (unsolicited email) filtering.

Instant messaging client:

- Preventing automatic loading of remote email images;
- Restricting file transfers.

Office productivity applications:

- Restricting macro (a special purpose command that provides a short-cut for a sequence of repeatable keystrokes or actions) use to permit macros only from trusted locations or which prompt the user to approve or reject each attempt to run a macro;
- Limiting personal information, such as name, initials, mailing address, and phone number, stored with each document created to that which is specifically required;
- Using secured folders for saving documents and holding temporary files, including auto-save and backup copies of documents; and
- Automatically and/or manually deleting documents which are no longer required.

Remote Access Software Configuration

If telework users are required to install remote access software onto their information assets or configure software built into the information asset's operating system, this software shall be configured based on the agency's requirements and recommendations. Remote access software shall be configured so that only the necessary functions are enabled. Telework users shall also ensure that whenever updates to the remote access software are available, that they are acquired and installed. If the agency provides the updates, the telework user shall take the appropriate action (such as install the update) in a timely manner when updates are available.

Security Maintenance and Monitoring

Telework users shall maintain their information assets' security on an ongoing basis, at a minimum once a month, including:

- Confirming periodically that the operating system and primary applications are up-to-date;
- Checking the status of security software periodically to ensure that it is still enabled, configured properly, and up-to-date;
- Creating a new user account whenever another individual needs to start using the information asset, as well as disabling or deleting a user account whenever the associated individual no longer needs to use the information asset. All the user accounts shall be reviewed periodically to ensure that only the necessary accounts are enabled;

- Changing the user’s system account and remote access passwords regularly;
- Periodically checking for potential security issues on the information asset (e.g., running utilities that check the computer for potential problems); and
- Investigating any cases in which the information asset begins to display unusual behavior.

Restrictions and Security with Use of Third Party Devices

Telework users shall consider the security risks related to the environment/location of a third-party device (e.g., public kiosks, such as hotel business centers) before deciding whether or not to use it. Users shall also consider who is responsible for securing a third-party device and who can access the device.

Telework users shall not use any third-party devices for performing sensitive functions or accessing confidential, personal or sensitive information.

Securing Personal Networks

Securing Wired Personal Networks

Personal networks can be wired or wireless. A wired network requires use of a cable between the computing device and cable modem. The telework user shall take the following precautions before connecting to a state agency IT infrastructure from an information asset attached to a wired personal network:

Separate the personal network from the Internet Service Provider's (ISP) network with a security device between the two, such as a broadband router, cable modem router, DSL router or a firewall appliance capable of enforcing the required network security policy.

1. This security device shall be configured to prevent computers outside the personal network from initiating communications with any of the devices on the personal network, including the telework device.
2. A firewall appliance or broadband router shall also be used to provide an additional layer of security, even if each device uses a personal firewall.
3. When installing and configuring firewall appliances or broadband routers, users shall perform the security precautions described in the manufacturer’s documentation, including:
    a. Changing default passwords on the device;
    b. Configuring the device so that it cannot be administered from outside the personal network;
    c. Configuring the device to silently ignore unsolicited outside connection attempts unless properly authenticated access is required by the ISP to support necessary communications with the IP’s infrastructure;
    d. Checking for software updates and applying them periodically, as explained in the manufacturer’s documentation—either automatically (typically daily or weekly) or manually (to be performed by the user at least monthly); and
    e. For broadband routers, turning off or disabling built-in wireless access points (AP) which are not used.

Securing Wireless Personal Networks

A wireless network uses electromagnetic waves instead of a cable to carry the signal over the communication path. The telework user shall take the following precautions before connecting to state agency IT infrastructure from an information asset attached to a wireless personal network:

1. Use strong encryption over the wireless network to protect communications. Configure the wireless network to use one of the following security protocols in order of decreasing preference:
    a. Wi-Fi Protected Access 2 (WPA2), with Advanced Encryption Standard (AES);
    b. WPA with AES; or
    c. WPA with Temporal Key Integrity Protocol (TKIP).

    (WEP is NOT an authorized encryption protocol)
2. Use a long and complex key length;
3. Only permit access for specified wireless network cards;
4. Change the default service set identifier (SSID);
5. Disable SSID broadcasts from the wireless access point; and
6. Disable Access Point (AP) administration through wireless communications.
7. Change the default administrative password to a unique strong password.

The US-CERT online reading room provides free less technical resources to assist individuals with securing wireless networks at http://www.us-cert.gov/reading_room/Wireless-Security.pdf